REVISTA
ILUSTRAÇÃO

A RESPONSABILIZAÇÃO DECORRENTE DO TRATAMENTO DE DADOS PESSOAIS E O SISTEMA SANCIONATÓRIO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS ("LGPD")

RESPONSIBILITY ARISING FROM THE PROCESSING OF PERSONAL DATA AND THE SANCTIONATORY SYSTEM OF THE GENERAL PERSONAL DATA PROTECTION LAW ("LGPD")

Camila Maria de Moura Vilela

Universidade de Lisboa, Lisboa, Portugal. E-mail: camilavilela@campus.ul.pt

Christine Mattos Albiani Lemos

Instituto Brasileiro de Mercado de Capitais, Rio de Janeiro, RJ, Brasil E-mail: kittyalbiani@gmail.com

DOI: https://doi.org/10.46550/ilustracao.v1i2.17

Recebido em: 11.11.2020

Aceito em: 04.12.2020

Resumo: Este artigo pretende analisar a responsabilização administrativa e, o posicionamento do judiciário, perante a atuação dos agentes de tratamento de dados pessoais, denominados como controlador e operador. Destacando a problemática que trata das sanções administrativas que terão aplicabilidade apenas a partir de 1º de agosto de 2021. Para tanto, buscaremos analisar o papel da Autoridade Nacional de Proteção de Dados ("ANPD") na efetivação das sanções administrativas e observar o tratamento, compartilhamento e fluxo de dados no Brasil, bem como as decisões judiciais proferidas até o momento devido a falhas de segurança da informação e danos aos titulares. O objetivo final das autoras é perquirir a forma de responsabilização decorrentes do tratamento de dados pessoais no país com a eficácia da LGPD.

Palavras-chave: Proteção de Dados. LGPD. Responsabilidade. Obrigações.

Abstract: This article intends to analyze the administrative accountability and, the position of the judiciary, before the performance of the personal data processing agents, called as controller and operator. Highlighting the problem that deals with administrative sanctions that will only apply from August 1, 2021. To that end, we will seek to analyze the role of the National Data Protection Authority ("ANPD") in the implementation of administrative sanctions and observe the treatment, data sharing and flow in Brazil, as well as the judicial decisions handed down so far due to information security flaws and damage to data subjects. The authors' ultimate goal is to investigate the form of accountability resulting from the processing of personal data in the country with the effectiveness of the LGPD.

Keywords: Data Protection. LGPD. Responsibility. Obligations.

Revista Ilustração | Cruz Alta | v. 1 | n. 2 | p. 57-67 | maio./agos. 2020.
DOI: https://doi.org/10.46550/ilustracao.v1i2.17

1 Introdução

O presente artigo pretende perquirir a responsabilização administrativa dos agentes de tratamento de dados pessoais (controlador e operador), em razão de violações à Lei Geral de Proteção de Dados Pessoais ("LGPD"), levando-se em consideração a sanção do Projeto de Lei nº. 1.179/2020 (agora a Lei nº. 14.010/2020), confirmando a vigência dos artigos 52, 53 e 54 da LGPD – que tratam das mencionadas sanções administrativas - com aplicabilidade apenas para 1º de agosto de 2021. Para tanto, irá se perquirir o papel da Autoridade Nacional de Proteção de Dados ("ANPD") na efetivação das sanções administrativas e observar o tratamento, compartilhamento e fluxo de dados no Brasil.

O objetivo geral da lei de proteção de dados é garantir que a tratamento das informações pessoais seja projetado para salvaguardar os indivíduos. Para evitar usos antiéticos dos dados pessoais, a proteção de dados distingue entre as finalidades permitidas e não permitidas.

Inicialmente, portanto, analisamos o contexto do regime jurídico do tratamento de dados pessoais em que se insere a LGPD, que ganha destaque quando se observa a sociedade da informação, perpassando pela importância atinente à privacidade e proteção de dados pessoais, neste contexto, a fim de justificar a escolha do presente trabalho.

Buscou-se salientar os fatores fundamentais que garantem o protagonismo da proteção de dados pessoais no panorama socioeconômico atual. A popularização da internet, o advento do *big data* e o desenvolvimento da inteligência artificial são alguns dos pilares da sociedade contemporânea e, portanto, a proteção de dados pessoais se torna cada vez mais relevante à medida que a quantidade de dados criados e armazenados continua a crescer.

Através da análise do sistema sancionatório instituído pela LGPD pretendeu-se analisar pormenorizadamente como irá se dar também a responsabilização das organizações diante da aplicabilidade da lei. Para tanto deve-se observar que seu escopo de aplicação atinge todas as instituições públicas e privadas que realizem tratamento de dados pessoais, sendo este entendido como toda a operação que envolva o dado pessoal (todo dado que identifique uma pessoa natural diretamente ou torne possível sua identificação).

Diante da constatação de que a LGPD é de aplicabilidade geral e ampla, tendo em vista que o mero acesso ao dado pessoal já é considerada uma operação de tratamento, seguido da coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento e até a eliminação do dado, afirma-se que a lei impõe obrigações de conformidade que devem ser cumpridas por organizações dos mais diversos segmentos da sociedade, sob pena de aplicação das mencionadas sanções administrativas e responsabilização.

Observa-se, nesta seara, a importância da adoção de Programas de Governança de Dados Pessoais – que visam encaminhar a organização para uma transformação perene de sua cultura de privacidade e segurança da informação –, que não só são incentivados pela LGPD, mas podem influir nas sanções administrativas, através de um abrandamento da pena imposta.

Através desta abordagem de Governança, possibilita-se construir regras internas de conformidade com a LGPD, apoiadas em pilares fundamentais de Compliance – como: o registro e acompanhamento de operações, análise de riscos (*risk assessment*), gerenciamento de controles internos, monitoramento, elaboração de manuais de conduta e projetos de melhoria

contínua –, que devem ser observados pelos seus colaboradores e refletidos nas atividades que envolvam o tratamento de dados pessoais.

O tema em questão possui grande relevância prática, e a adoção das regras e sanções que visam assegurar a privacidade de dados pessoais e a segurança da informação tendem a facilitar o fluxo desses dados nas transações comerciais.

As discussões apresentadas serão constituídas por meio de uma abordagem descritiva e de caráter qualitativo, sendo imprescindível o recurso à pesquisa bibliográfica e documental, para se delimitar os contornos da responsabilidade dos agentes de tratamento de dados nestas operações, bem como das organizações que realizam esse tratamento, sobretudo, quando se observa que algumas ações judiciais já estão sendo propostas no âmbito nacional.

2 O regime jurídico do tratamento de dados pessoais

A privacidade é um dos conceitos mais importantes dentro da sociedade da informação, mas também um dos mais elusivos. À medida que a tecnologia em rápida mudança torna as informações cada vez mais disponíveis, acadêmicos, ativistas e formuladores de políticas têm se esforçado para definir a privacidade e a proteção às informações pessoais.

Nesta sede, a LGPD, a legislação brasileira que regula as atividades de tratamento de dados pessoais, trouxe visibilidade para a intimidade e privacidade sobre as informações pessoais. Inobstante esses direitos fundamentais serem de extrema relevância para o contexto abordado, vale destacar que as leis de proteção de dados pessoais não são leis apenas voltadas para pontos de privacidade. A LGPD, por seu turno, é voltada para proteger direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Ao longo da história moderna, desde pesquisas, *big data* e vigilância em massa, a noção de privacidade tem surgido repetidamente. No entanto, conceituar a privacidade não é uma tarefa fácil e, embora o termo 'privacidade' sempre tenha permanecido o mesmo, seu significado nunca parou de evoluir.

Temos de estar conscientes dessa evolução, se quisermos enfrentar eficazmente os desafios futuros, em particular a questão premente da regulamentação da coleta, do acesso e da utilização de informações pessoais, tanto por parte de intervenientes privados como públicos.

Assim esclarece Danilo Doneda[1]:

> Por difícil que seja cristalizar a problemática da privacidade em um único conceito, é, no entanto, razoavelmente natural constatar que ela sempre foi diretamente condicionada pelo estado da tecnologia em cada época e sociedade. Podemos inclusive aventar a hipótese de que o advento de estruturas jurídicas e sociais que tratam do problema da privacidade são respostas a uma nova condição da informação, determinada pela tecnologia.

A internet, por exemplo, é uma das áreas em que a privacidade informacional, a proteção de informações pessoais, se tornou crucial. As preocupações com a privacidade estão, hoje em dia, focadas em grande medida nas informações que compartilhamos ou geramos na internet, muitas vezes publicamente, ao invés do que desejamos ocultar dentro dos limites privados das nossas casas.

1 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006. p. 60.

Revista Ilustração | Cruz Alta | v. 1 | n. 2 | p. 57-67 | maio./agos. 2020.
DOI: https://doi.org/10.46550/ilustracao.v1i2.17

Nesse sentido, a importância da proteção de dados pessoais aumenta à medida que a quantidade de dados criados e armazenados continua a crescer. Conforme já indicado, existe uma ligação entre os conceitos de privacidade e proteção de dados.

Geralmente, privacidade e proteção de dados são conceitos sociais que, desde o início, transmitem a ideia de que as pessoas têm direito a algum tipo de autonomia e proteção no que diz respeito à sua vida privada e pessoal. A ideia principal é que uma pessoa é mais do que apenas um aspecto da sociedade e, consequentemente, é algo em seu próprio direito. Ao analisarmos de um ponto de vista jurídico, a questão é como a privacidade e a proteção de dados podem ser promovidas à compreensão dos diplomas legais.

A importância dos direitos de informação tende a crescer, busca-se, então, um equilíbrio entre a privacidade, a vida privada e os dados pessoais. No Brasil, o quadro jurídico em matéria de proteção de dados passou a ser repensado a partir do ponto de vista técnico da aplicabilidade da LGPD, além da perspectiva institucional, ou seja, através desse cenário organizações e tribunais estão desenhando novas linhas sobre a matéria, traçando um novo panorama acerca dos nortes gerais da proteção de dados pessoais e sua aplicabilidade.

Destacamos ainda, que o Código de Defesa do Consumidor ("CDC") em si é um microssistema de proteção de dados pessoais, por trazer certas obrigações e princípios voltados para a relação de consumo, como o princípio da boa-fé e da transparência e, um elemento essencial da boa-fé objetiva é o dever de informação.

Acresce que, a legislação nacional de proteção de dados pessoais oferece maiores garantias aos brasileiros, como os direitos dos titulares, bases legais para o tratamento, princípios norteadores, agentes de tratamentos, responsabilidade do responsável pelo tratamento, entre outros pontos.

Para que os titulares dos dados possam exercer os seus direitos e para que a autodeterminação informativa funcione na prática, os cidadãos, na sua qualidade de titulares de dados, devem ser capazes de descobrir quais os dados pessoais armazenados sobre eles, ter acesso a esses dados, e saber como isso é processado e com quem é compartilhado.

Sublinhe-se também que há figuras que são responsáveis pelo tratamento, que lhe são atribuídas obrigações e responsabilidades. Assim, com base nos princípios e nortes da LGPD, os agentes de tratamento devem ter em conta as técnicas, contextos e finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades dos titulares.

Portanto, dentro dessa análise, apresenta-se a necessidade e importância do nosso país cumprir com os padrões mínimos, para ser considerado um país confiável para, por exemplo, ter relações comerciais quanto a transferência de dados pessoais, para que possa realizar o tratamento de dados pessoais de cidadãos de todo o mundo e, por isso, a figura dos agentes também torna-se algo em destaque, bem como a sua responsabilização.

3 Os responsáveis pelo tratamento de dados pessoais

No que toca ao assunto, a LGPD é voltada para proteger direitos fundamentais, políticos e do estado democrático do direito, está para proteger o indivíduo, não o policiar. A questão é sempre qual é o escopo e o propósito da coleta e tratamento de dados. Isso se aplica a empresas, entidades legais, não aos indivíduos – salvo se houver finalidade comercial.

Em termos gerais, é importante que as organizações tenham diretrizes internas de privacidade e segurança quanto ao tratamento dos dados pessoais. Para tanto, o tratamento entende-se como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Organizações públicas, estatais ou não estatais e entidades privadas total ou parcialmente pertencentes ao estado, bem como entidades privadas que processam dados confidenciais como seu negócio principal e aquelas que processam grandes volumes de dados, devem designar um encarregado para a proteção de dados pessoais.

De acordo com a LGPD, os agentes de tratamento são o controlador e o operador, essas figuras têm-se destaque no capítulo VI da LGPD, além de outros artigos e incisos. O responsável pelo tratamento, a quem compete as decisões referentes ao tratamento de dados pessoais é denominado como controlador, por sua vez, o operador é quem realiza o tratamento dos dados pessoais em nome do controlador. Ressaltamos ainda que, tanto o controlador quanto o operador, podem ser pessoa natural ou jurídica. É de suma importância essa distinção, visto que é ao responsável pelo tratamento que incube assegurar a observância das obrigações legais em matéria de proteção de dados[2].

Trazemos o seguinte exemplo, uma companhia de teatro em Recife, Pernambuco, coleta dados dos assinantes de seu boletim informativo por meio de seu website. O site é hospedado em um provedor de hospedagem em nuvem local, incluindo todos os dados das assinaturas da empresa. Quando uma pessoa deseja cancelar a assinatura do boletim informativo, o provedor de hospedagem em nuvem é instruído pela companhia teatral a excluir os dados em 30 (trinta) dias.

Nesse exemplo, a companhia de teatro é a controladora de dados e o provedor de hospedagem em nuvem é o operador. Ambas as partes estão no Brasil, e, portanto, devem cumprir a LGPD.

Trazemos outro exemplo em que a coleta e o processamento de dados estão fora do escopo material, como uma lista de contatos no telefone pessoal, com fotos, datas de nascimento, e mensagens que são muito particulares do titular. A este respeito, nota-se dois cenários, o primeiro que envolve a comercialização dos dados pessoais e, portanto, engloba outros agentes nessa relação de tratamento desses dados pessoais, e outro onde os dados pessoais não são objeto dessa relação mercantil.

Outra figura que destacamos é a do encarregado, e uma das principais questões alocadas sobre o tema é: todas as empresas ou entidades devem ter um encarregado? A resposta é não, como pode se evidenciar da redação do art. 41 da LGPD que traz essa obrigação somente para os controladores. As funções do encarregado, por sua vez, estão descritas no § 2º, do artigo 41, destacando-se entre as principais funções a de comunicar-se com os titulares dos dados pessoais, interagir e cooperar com a ANPD, orientar os colaboradores da organização quanto às boas práticas e executar as atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

2 LOPES, Teresa Vale. *Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados.* In: COUTINHO, Francisco Pereira; MONIZ, Graça Canto. Anuário da Proteção de Dados 2019. Lisboa: Cedis, 2019. p. 58

Revista Ilustração | Cruz Alta | v. 1 | n. 2 | p. 57-67 | maio./agos. 2020.
DOI: https://doi.org/10.46550/ilustracao.v1i2.17

Ademais, salientamos que o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no artigo 43 da Lei.

Outro ponto com relação a responsabilidade e o ressarcimento de danos é que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Sob os aspectos relativos à responsabilização, devemos observar as possibilidades que são suscetíveis de gerar alterações na dinâmica de negociação dos contratos a serem celebrados entre os responsáveis pelo tratamento e o encarregado, designadamente no que respeita à transferência de risco e ações de regresso entre essas figuras.

O encarregado, por sua vez, pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Portanto, é igualmente importante considerar os riscos que podem resultar da relação entre controlador, operador e encarregado.

Por seu turno, em caso de ocorrer danos aos titulares de dados, a organização poderá ser responsabilizada judicialmente, ficando sujeita ao pagamento de multa e outras medidas, até mesmo equiparadas às sanções administrativas descritas na Lei, conforme o exposto a partir do artigo 52.

A nível nacional, os tribunais passam a tenra esclarecer os aspectos problemáticos da interpretação da legislação nacional. Em outro ponto, investigadores desta temática traçam uma doutrina sobre o tema. Ao nosso, a aplicabilidade do princípio da proporcionalidade, é o ponto chave de toda a discussão na distinção entre o interesse público e privado, portanto, deve ser um dos aspectos preponderantes quando se discute as tratativas sobre proteção de dados pessoais.

Por fim, cumpre salientar que haverá situação que as organizações determinarão em conjunto os meios e fins do processamento, tornando-se então, controladores conjuntos, conhecido como co-controladores (ante a normatividade do GDPR, não havendo equivalente expresso na LGPD). Neste caso, essa figura possui um certo grau de flexibilidade na distribuição e atribuição de obrigações e responsabilidades, mas, como regra geral, serão solidariamente responsáveis pelo cumprimento em relação ao titular dos dados.

Assim, é fundamental alcançar um equilíbrio que garanta o cumprimento das regras de proteção de dados e, ao mesmo tempo, evite a multiplicação de controladores que podem levar à falta de clareza.

4 Sanções administrativas e a responsabilização dos agentes de tratamento de dados pessoais e organizações

A preocupação acerca da privacidade pelas instituições públicas e privadas, sobretudo, pelas empresas, se dá pelo fato de que a proteção de dados pessoais não é mais uma escolha, afinal, a adequação aos seus ditames se tornou cogente por força de lei.

Diante deste cenário de obrigatoriedade de observação do regramento da LGPD numa interpretação sistemática com as outras normas que regem a proteção de dados pessoais no país,

realiza-se o seguinte questionamento: Os agentes são responsáveis pelo tratamento de dados pessoais que realizam? Em caso de descumprimento da lei quais sanções podem ser aplicadas? Em que medida as organizações respondem administrativa ou judicialmente?

Sabendo que a LGPD considera tratamento de dados pessoais toda e qualquer operação que envolva o dado pessoal, até mesmo o mero acesso, que tornam possível a identificação do titular – através de números (como RG e CPF), e-mail corporativo, características pessoais, registros de localização, identificação eletrônica (como IP e Cookie), qualificação pessoal, dados genéticos, biometria, etc. – necessita-se frisar a preocupação da adequação à lei de organizações de todos os setores.

Observando-se o panorama de aplicabilidade geral e horizontal da LGPD, afirma-se que este diploma normativo será amplamente aplicado, protegendo a privacidade dos titulares de dados pessoais em todos os setores econômicos e independentemente do tamanho da organização. É comumente dito, que a lei irá ter aplicabilidade desde uma empresa de pequeno porte, até uma organização que trabalhe exclusivamente com análise de dados.

A ANPD, neste contexto, terá dentre suas funções a de delimitar uma aplicação proporcional, ponderada, entre instituições distintas e entre segmentos distintos da sociedade.

Cumpre salientar, neste âmbito, a constatação de que a coercitividade das leis têm sido muito associada à instrumentalização administrativa que o legislador confere aos órgãos de fiscalização, notadamente componentes do Poder executivo, a quem compete o poder de polícia[3].

Demonstra-se, portanto, a relevância do papel da ANPD na aplicação das sanções administrativas disciplinadas nos artigos 52, 53 e 54 da LGPD – que tratam das mencionadas sanções administrativas – que tiveram sua aplicabilidade postergada para 1º de agosto de 2021, com a sanção do Projeto de Lei nº. 1.179/2020 (agora a Lei nº. 14.010/2020).

Trata-se de constatação inequívoca, portanto, que se houve o tratamento de dados pessoais e a atividade não estiver sob a égide de nenhuma das exclusões previstas na lei, todas as organizações (públicas ou privadas), estão sujeitas às regras da LGPD e devem buscar, o quanto antes, soluções para se adequarem à legislação, pois se violarem seus preceitos, se submeterão às suas sanções, vigentes a partir de agosto de 2021.

A LGPD elenca dez princípios (no artigo 6º) que são verdadeiros alicerces e subsídios da efetividade dos objetivos pretendidos pela lei, constituindo os pilares fundamentais da proteção de dados no país. Cumpre salientar que inobstante serem princípios, e, portanto, possuírem algum grau de abstração, são comumente complementados por regras instituídas pela própria norma. Garante-se, dessa forma, efetividade e objetividade ao se analisar seu cumprimento ou incumprimento, sobretudo para fins de aplicação de penalidades.

Para análise da temática pertinente ao presente trabalho, destacam-se os princípios da responsabilização e prestação de contas. Ao lado dele, a lei também elenca o princípio da segurança e prevenção que possuem uma relação simbiótica entre si. Nesse sentido, afirma-se que a responsabilidade vai depender muito da segurança e das medidas de prevenção que os agentes de proteção de dados pessoais adotarem.

Fato é que os setores de Compliance e Cybersegurança nunca foram tão importantes no

3 ALVES, Fabricio da Mota. *Das sanções administrativas.* In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, Revista dos Tribunais, 2019, p. 362.

Revista Ilustração | Cruz Alta | v. 1 | n. 2 | p. 57-67 | maio./agos. 2020.
DOI: https://doi.org/10.46550/ilustracao.v1i2.17

ambiente empresarial e Programas de Governança de Dados Pessoais tornaram-se verdadeiros aliados para que haja a efetiva adequação à lei e prevenção de riscos e responsabilização.

O regime sancionatório instituído na LGPD pode ser considerado inovador para a disciplina normativa brasileira, trazida de acordo com o modelo europeu e pretende garantir efetividade à lei, sobretudo, a partir da aplicação das seguintes sanções administrativas:

(i) Advertência: deve conter um prazo para adequação do tratamento tido como irregular;

(ii) Multa simples: pode chegar a 2% do faturamento da empresa, até 50 milhões de reais por infração. Ou seja, se tiver mais de uma infração, esse valor pode ser acumulado;

(iii) Multa diária;

(iv) Publicação da infração: pode impactar de forma muito negativa a organização, sobretudo, por ser considerada uma propaganda negativa e afetar a confiabilidade da empresa perante seus consumidores e fornecedores;

(v) O bloqueio dos dados pessoais a que se refere a infração, ou, até mesmo a eliminação dos dados pessoais: Esta medida que pode inviabilizar diversos modelos de negócios que dependem desse tratamento de dados pessoais.

Cumpre observar que existem critérios para aplicação das referidas sanções, conforme o §1º do artigo 52 da LGPD, quais sejam: a gravidade e a natureza das infrações e direitos afetados; a boa-fé do infrator; vantagem econômica do infrator; eventual reincidência; o grau do dano; a cooperação do infrator; a adoção reiterada e demonstrada de medidas de segurança e de procedimentos internos capazes de mitigar os riscos; adoção de política de boas práticas e um plano de governança; pronta adoção de medidas corretivas e proporcionalidade entre a gravidade da infração e a intensidade da sanção.

Diante da impossibilidade de aplicação das mencionadas sanções administrativas até agosto de 2021 pela ANPD - que exercerá o importante papel fiscalizatório e regulador da LGPD - através da observância de procedimento administrativo que respeite o contraditório, imprescindível se faz destacar o papel do Judiciário na efetivação das obrigações, princípios e regras instituídos pela lei.

Cumpre observar que a responsabilização civil dos agentes de tratamento de dados pessoais ocorrerá de acordo com a necessidade de observância das obrigações instituídas pela LGPD, aplicando-se os elementos tradicionais da responsabilidade civil: ilicitude, dano e nexo de causalidade, conforme artigo 42 da lei.

Deve-se ressaltar que a LGPD não é propriamente clara ao estabelecer o regime de responsabilização civil, se subjetiva (decorrente de conduta negligente, imprudente ou imperita) ou objetiva (independentemente de culpa do causador do dano).

Fato é que se houver uma relação de consumo, ou seja, se constatar-se incidente de dados pessoais o qual se causou danos aos consumidores, aplica-se a teoria do risco da atividade, fazendo incidir o regime de responsabilização objetiva do CDC (artigos 12 a 14) estabelecido para os envolvidos na cadeia de consumo, bem como a possibilidade de inversão do ônus da prova.

Em versões anteriores do Projeto de Lei que deu origem à LGPD chegou a se incluir disposições que conceituavam a atividade de tratamento de dados pessoais como atividade de risco, expressamente, as quais, no entanto, foram retiradas da proposição no decorrer do processo

legislativo[4].

Diante deste contexto, afirma-se que quando tratar-se de relação civil, é possível sustentar a aplicação da regra geral da responsabilidade subjetiva com culpa presumida, já que o artigo 42, §2º da LGPD evidencia a aplicabilidade da teoria dinâmica do ônus da prova, fazendo com que tal ônus recaia sobre aquele que possui melhores condições para se desincumbir do ônus da prova.

Exemplificando a importância do papel do Judiciário no contexto ora exposto, aponta-se, a sentença proferida no Processo n. 1080233-94.2019.8.26.0100, em 29/09/2020, proveniente da 13º Vara Cível do Tribunal de Justiça do Estado de São Paulo, em desfavor da empresa Cyrela Brazil Realty S/A Empreendimentos e Participações.

Na sentença, a Cyrela, companhia do ramo imobiliário, foi condenada a indenizar em R$ 10 mil (dez mil reais) um cliente que teve informações pessoais enviadas para outras empresas. No referido caso, o Autor comprou um apartamento em novembro de 2018. No mesmo ano, ele começou a ser importunado por instituições financeiras e firmas de decoração, que citavam sua recente aquisição com a parte ré[5].

Um outro caso emblemático[6] foi o que envolveu o Mercado Livre. No Processo n. 0733785-39.2020.8.07.000, o autor - o Ministério Público do Distrito Federal e Territórios (MPDFT) - provou que o *e-commerce* atuou como intermédio de comercialização maciça de dados pessoais, ofertando a venda de cadastros e banco de dados em geral.

O Juiz da 17ª Vara Cível de Brasília deferiu a tutela de urgência para determinar que a empresa se abstivesse de disponibilizar, de forma gratuita ou onerosa, digital ou física, dados pessoais de quaisquer indivíduos, sob pena de multa de R$ 2 mil (dois mil reais) para cada operação.

Tal decisão foi fundada na violação aos ditames da LGPD e princípios constitucionais, dentre eles: o acesso à informação adequada acerca dos serviços que lhes são postos à disposição; privacidade; autodeterminação informativa, inviolabilidade da intimidade, da honra e da imagem, defesa do consumidor, direitos humanos, livre desenvolvimento da personalidade e dignidade.

Em 21 de setembro de 2020, o Ministério Público do Distrito Federal ajuizou a Ação Civil Pública em face de site que comercializava informações pessoais (nomes, e-mails, contatos para SMS, bairro, Cidade, Estado e CEP's de usuários) de 500.000 (quinhentas mil) pessoas naturais da cidade de São Paulo, por meio de site na internet. Segundo alegação do Autor, o site vendia as informações segmentadas de acordo com diferentes perfis.

A ação estava fundada na tutela constitucional de proteção à vida privada e à intimidade, a qual decorre a proteção de dados pessoais, direitos que garantem ao titular o controle sobre seus próprios dados pessoais e foi extinta sem resolução de mérito pela ausência de condição da ação.

---

4 BRUNO, Marcos Gomes da Silva. *Dos Agentes de Tratamento de Dados Pessoais.* In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, Revista dos Tribunais, 2019, p. 327.

5 ANGELO, Tiago. *Juíza aplica LGPD e condena construtora que não protegeu dados de cliente.* Conjur, 30/09/2020. Disponível em: <https://www.conjur.com.br/2020-set-30/compartilhar-dados-consumidor-terceiros-gera-indenizacao>. Acesso em: 10/10/2020.

6 Site Legal Cloud. 5 Decisões Judiciais sobre a LGPD nos Tribunais [2020]. Disponível em: < https://legalcloud.com.br/decisoes-judiciais-lgpd-tribunais/> . Acesso em: 11/11/2020.

Revista Ilustração | Cruz Alta | v. 1 | n. 2 | p. 57-67 | maio./agos. 2020.
DOI: https://doi.org/10.46550/ilustracao.v1i2.17

Recentemente, em 20 de novembro de 2020, foi proferida uma decisão em sede de tutela antecipada, determinando a suspensão da venda de dados pessoais de consumidores pela empresa Serasa Experian, sob pena de multa diária, derivada de ação civil pública ajuizada pela Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec) vinculada ao Ministério Público do Distrito Federal ("MPDF")[7].

A entidade verificou durante investigações que a empresa comercializa informações como nome, endereço, CPF, número de telefone, localização, perfil financeiro, poder aquisitivo e classe social para outras companhias, a fim de que esses dados sejam usados para publicidade e captação de novos clientes. Tais informações seriam vendidas por 98 centavos por pessoa e estima-se que cerca de 150 milhões de brasileiros tenham tido seus dados tratados de forma irregular diante dessas vendas, sem observância das diretrizes e princípios trazidos pela lei.

Ante os casos práticos supracitados, evidencia-se a necessidade de adoção de critérios delineados de responsabilização decorrente da violação dos ditames estabelecidos na LGPD pelo Judiciário, de modo a garantir segurança jurídica e dar efetividade à lei, por meio da responsabilização dos agentes de tratamentos de dados pessoais de acordo com suas obrigações.

5 Considerações finais

Diante da análise do panorama atual de proteção de dados pessoais no Brasil, com a verificação da importância da temática na sociedade informacional, das obrigações atinentes às figuras do controlador e do operador e das sanções administrativas e responsabilização referentes à inobservância dos preceitos instituídos na LGPD, pode-se concluir pela necessidade de uma mudança de cultura das organizações que realizam o tratamento desses dados.

Verifica-se a premente necessidade de implementação de Programas de Compliance em Privacidade de Dados Pessoais para que haja a conformidade das atividades empresariais com a lei e uma transformação perene da cultura organizacional, focada na prevenção de riscos e responsabilização, sobretudo, porque vislumbra-se um cenário de incertezas quanto à aplicabilidade das sanções administrativas atinentes às violações da lei, pela ANPD, que só poderão ocorrer a partir de agosto de 2021.

Dessa forma, o Poder Judiciário exercerá o papel fundamental de garantir a plena eficácia da lei, especialmente, quando se observa a proteção da privacidade, intimidade e autodeterminação informativa – controle do cidadão sobre a coleta dos seus dados –, como direitos fundamentais reconhecidos pelo Supremo Tribunal Federal.

Ressalta-se, portanto, o papel das decisões judiciais que irão delimitar os contornos da responsabilização das organizações no tratamento dos dados pessoais no país, sendo necessária a adoção de critérios razoáveis, que levem em consideração os aspectos apontados pela LGPD, como a gravidade e a natureza das infrações e direitos afetados; a boa-fé do infrator; vantagem econômica auferida; eventual reincidência; o grau do dano e adoção de política de boas práticas.

Este delineamento dos contornos da responsabilização das organizações que realizam o tratamento de dados pessoais, controladores e operadores, deverá ocorrer de forma a garantir segurança jurídica aos envolvidos nesta relação, possibilitando alguma previsibilidade quanto às

7 Exame. MPDFT suspende venda de dados pela Serasa Experian por violação à LGPD. Disponível em: <https://exame.com/tecnologia/mpdft-suspende-venda-de-dados-pela-serasa-experian-por-violacao-a-lgpd/>. Acesso em: 24/11/2020.

consequências de irregularidade no tratamento de dados pessoais, e de dar efetividade à lei.

O Judiciário, portanto, quando for acionado e enquanto não houver a possibilidade de aplicação das sanções administrativa, terá a incumbência de estabelecer os limites razoáveis do que é considerado um legítimo tratamento de dados pessoais pelas organizações, diante da sistemática de proteção instituída pela LGPD, buscando compatibilizar a aplicação concreta dos princípios, bases legais, finalidades e regras de proteção de dados pessoais no caso concreto, com a livre iniciativa, e o desenvolvimento da inovação, sem se tornar um óbice aos novos modelos de negócio e novas tecnologias.

Referências

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

ALVES, Fabricio da Mota. Das sanções administrativas. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, Revista dos Tribunais, 2019.

ANGELO, Tiago. *Juíza aplica LGPD e condena construtora que não protegeu dados de cliente.* Conjur, 30/09/2020. Disponível em: https://www.conjur.com.br/2020-set-30/compartilhar-dados-consumidor-terceiros-gera-indenizacao. Acesso em: 10/10/2020.

BRUNO, Marcos Gomes da Silva. Dos Agentes de Tratamento de Dados Pessoais. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, Revista dos Tribunais, 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006.

EXAME. MPDFT suspende venda de dados pela Serasa Experian por violação à LGPD. Disponível em: https://exame.com/tecnologia/mpdft-suspende-venda-de-dados-pela-serasa-experian-por-violacao-a-lgpd/.

LEGAL CLOUD. *5 Decisões Judiciais sobre a LGPD nos Tribunais [2020].* Disponível em: https://legalcloud.com.br/decisoes-judiciais-lgpd-tribunais/.

LOPES, Teresa Vale. Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados. In: COUTINHO, Francisco Pereira; MONIZ, Graça Canto. *Anuário da Proteção de Dados 2019*. Lisboa: Cedis, 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, Revista dos Tribunais, 2019.